UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 900 West Temple St. Apt. 528 Los Angeles, CA 90012	)	Case No. 19-MJ-133

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1014	False Statement To A Bank
18 U.S.C. § 1344	Attempted Bank Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

See Attached Affidavit.

Applicant's signature

Aundria Davis Ly, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date:

Judge's signature

City and state: Los Angeles

Printed name and title

AUSA: Devon A. Myers ((213) 894-0649)

ATTACHMENT A-1

PREMISES TO BE SEARCHED:

The premises to be searched is 900 West Temple Street, Apartment 528, Los Angeles, CA 90012. The premises is located in Los Angeles County. It is a multi-story apartment complex with beige exterior paint with wrought iron balconies. The apartment building is located on the westside of North Fremont Avenue at Temple Street. Unit #528 is located on the fifth floor. The door is beige and the number “528” are affixed to the wall just east of the location above the doorbell. The SUBJECT PREMISES includes any parking spaces, garages, storage spaces, and appurtenances exclusively assigned to Apartment 528. It also includes any vehicles or persons inside the SUBJECT PREMISES.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1014 (False Statement To A Bank); 18 U.S.C. § 1344 (Attempted Bank Fraud); and 18 U.S.C. § 1028A (Aggravated Identity Theft) (the "Subject Offenses"), namely:

a. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than DARIUS BURKS ("BURKS") or any other resident of the SUBJECT PREMISES, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers.

b. Records, documents, programs, applications, or materials pertaining any bank accounts, credit card accounts, or other financial accounts, including applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

c. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

d. Any altered, counterfeit, or fraudulent identifications, checks, access devices, monetary instruments, or other official documents;

e. Any identifications, checks, access devices, monetary instruments, or other official documents that are not addressed to, or in the name of, BURKS or any other resident of the SUBJECT PREMISES.

f. Any tools or equipment, such as computers, software, printers, scanners, embossing machines, credit card readers or encoders, washing chemicals, or imprinting tools, used or intended to be used to alter, counterfeit, or create fraudulent checks, access devices, or other monetary instruments;

g. Records of off-site storage locations, including safe-deposit box keys, records, receipts, or rental agreements for storage facilities;

h. Indicia of occupancy, residency or ownership of the SUBJECT PREMISES and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, lease of rental agreements, addressed envelopes, keys, letters, mail, canceled mail envelopes, or clothing;

i. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

k. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

l. Any records, documents, programs, applications or materials that facilitate the procurement of identification information;

m. Any loan documents records, documents, programs, applications or materials submitted to a bank by BURKS that includes his correct information or false information;

n. Any communications, records, documents, programs, applications or materials related to the procurement of another person’s identity or efforts to submit false paperwork to any lending institution.

o. Any pay stubs related to BURKS’s employment from July 2015 to the present.

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

I. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, law enforcement personnel are authorized to: (1) depress BURKS's thumb- and/or fingerprints onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of BURKS's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, AUNDRIA DAVIS LY, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search:

a. The property located at 900 West Temple St., Apartment 528, Los Angeles, California 90012 (the "SUBJECT PREMISES"), as described further below and in Attachment A-1, which is incorporated herein by reference.

b. The person of DARIUS BURKS ("BURKS"), as further described in Attachment A-2, which is incorporated herein by reference, provided that BURKS is located within the Central District of California at the time of the search.

2. The requested warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1014 (False Statement To A Bank); 18 U.S.C. § 1344 (Attempted Bank Fraud); and 18 U.S.C. § 1028A (Aggravated Identity Theft) (collectively, the "SUBJECT OFFENSES"), as described in Attachment B, which is incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation

into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. AGENT'S BACKGROUND

4. I am currently assigned as a Task Force Officer ("TFO") at the Federal Bureau of Investigation ("FBI") where I work the Child Exploitation Task Force ("CETF"). I was deputized as a Deputy United States Marshal on April 20, 2017. I am also a sworn peace officer with the Los Angeles County District Attorney's Office, Bureau of Investigation, and have been since November 2014. I was previously employed by the Los Angeles Police Department from January 2011 to November 2014. During my law enforcement career, I have participated in numerous fraud-related investigations. During the investigation of these cases, I have participated in numerous arrests, executions of search warrants, and seizures of evidence. Since my assignment to the CETF, I have received both formal and informal training regarding cyber investigations. Through these means, I have learned about schemes and designs commonly used to commit financial-based crimes, as well as the practices that individuals who commit financial-based crimes employ while attempting to thwart law enforcement's efforts to effectively investigate those crimes.

III. SUMMARY OF PROBABLE CAUSE

5. As described in further detail below, in February 2018, BURKS attempted to purchase two BMW sedans from two separate car dealerships in Los Angeles County using a false

social security number ("SSN") on his financial documents when applying for car loans offered through federally insured financial institutions at these car dealerships. He also provided fictitious employment information and pay stubs. This fraud occurred while BURKS was on pretrial release for an unrelated case currently pending before the Honorable Terry J. Hatter, Jr. in United States v. Sutton et al., Case No. CR 14-407-TJH-2. Based on this conduct, on December 4, 2018, United States Magistrate Judge Jacqueline Chooljian issued a complaint and arrest warrant for BURKS in case number 2:18-MJ-3214.

6. At the time the complaint was filed, I was unable to determine where BURKS was living. I now know that he is living at the SUBJECT PREMISES. Given that BURKS filled out paperwork connected to the fraudulent loan statements and used someone else's SSN, I believe that there is probable cause that there will be evidence of the SUBJECT OFFENSES at the SUBJECT PREMISES or on digital devices recovered from BURKS's person.

IV. STATEMENT OF PROBABLE CAUSE

7. I know the following facts from conversations with and reviewing reports written by FBI Special Agent ("SA") Heng Liv, and from reviewing the documents obtained from the car dealerships related to BURKS's loan applications, and from my own investigation.

BURKS'S ATTEMPTED PURCHASE OF A BMW FROM GLENN THOMAS DODGE

8. On or about February 24, 2018, BURKS attempted to purchase a 2013 BMW 3 series sedan (the "2013 BMW") from Glenn E. Thomas Dodge Chrysler Jeep in Long Beach, California ("Dodge

Dealership"). BURKS bought the 2013 BMW with no money down and took the car home that day.

9. To obtain the car, BURKS provided: (1) information so that the Dodge Dealership could run a credit check; (2) a copy of his California driver's license ("CDL"); and (3) insurance information.

10. BURKS also needed to obtain financing, a service with which the Dodge Dealership routinely assists. BURKS submitted a loan application to the Dodge Dealership for $24,908.38, which the Dodge Dealership reviewed and then forwarded to Regional Acceptance Corp. ("RAC"), a subsidiary of Branch Bank and Trust ("BB&T"), a bank holding company that is insured by the Federal Deposit Insurance Corporation ("FDIC"). The application required BURKS to provide personal identifying information, including his address and SSN, as well as copies of his pay stubs and information about his income and his employer. The credit application that BURKS signed includes the language "I certify that I have read and agree to the terms of this application and that the information in it is complete and true."

11. Pursuant to their protocol, the finance managers at the Dodge Dealership reviewed BURKS's loan application and performed a credit check on BURKS. As documented in SA Liv's report, Alice Yu ("Yu"), one of the finance managers, recalled that she did a second review of the materials BURKS submitted and that BURKS's pay stubs did not "look good." Specifically,

Yu remembered that there was something about the withholdings and stub itself that did not look right to her.

12. Yu also reviewed BURKS's credit report and recalled that he had a credit score of around 700, which is considered good credit. She did note, however, that BURKS was only listed as an authorized user on other people's credit cards. (I know, from my training and experience, that persons preparing to perpetrate a fraudulent scheme will often list themselves as users on other peoples' credit accounts, if those credit accounts already have good standing, as a way to increase their own credit score.)

13. Even though Yu said that BURKS's application raised a red flag for her, Yu's manager approved the other finance manager, Cindy Kim, to proceed with BURKS's loan application. At that point, the Dodge Dealership forwarded the credit application to RAC and proceeded to enter into a contract with BURKS to purchase the 2013 BMW.

14. As documented on the loan application, BURKS provided his true name and date of birth, which is also contained on the driver's license that the Dodge Dealership made a copy of for its records. He also provided an SSN ending in 8374 (the "8374 Social"), an address on Atherton Street, in Long Beach, California (the "Long Beach Address"), home phone (424) 389-6875 ("BURKS's Home Number"), and business phone number (562) 556-0218. The pay stub that BURKS provided indicated that BURKS worked at Perpetual Holdings, Inc.

15. As SA Liv's report provides, Yu said that a couple of days later, RAC called the Dodge Dealership and requested more documents from BURKS. RAC indicated that it was unable to verify BURKS's employment because the phone number he had provided for his work did not have any person with whom an RAC representative could talk. RAC requested that the Dodge Dealership ask BURKS for a copy of his social security card. I do not know whether anyone contacted BURKS to make that request.

16. BB&T also filed a report documenting BURKS's suspicious loan application. That report noted that RAC determined that the paystub was fraudulent due to the format of the paystub and that the deductions set forth thereon were out of order.

17. RAC denied the loan because it was unable to verify BURKS's job, his pay stubs, and his SSN.

18. Because RAC declined the loan, the Dodge Dealership called BURKS and asked him to return the vehicle. According to Yu, he was agitated and initially refused to return the vehicle. A couple of days later, someone who claimed to be BURKS's brother dropped the vehicle at the dealership with the keys in the car.

19. Using law enforcement databases, I confirmed that BURKS's Home Number listed on the documents is subscribed to BURKS.

20. I have reviewed the signatures on the loan application and sale contract for the purchase of the 2013 BMW, and they appear identical to the signature on the CDL that BURKS provided

to the Dodge Dealership. I also know, from my training and experience, that if BURKS's appearance did not match the photograph depicted in the CDL, it is unlikely that the dealership would have moved forward with allowing him to purchase the car. As such, I believe that BURKS was the person who went to the Dodge Dealership to purchase the 2013 BMW.

BURKS'S ATTEMPTED PURCHASE OF ANOTHER BMW, THIS TIME FROM CARSON HONDA

21. Around the same time, BURKS attempted to purchase a 2012 BMW 740I (the "2012 BMW") from Carson Honda. Carson Honda submitted a loan application in the amount of $27,363.17, on BURKS's behalf to Santander Consumer USA Inc. ("Santander"), an FDIC-insured vehicle financing company specializing in automotive financing for car dealerships.

22. Santander provided copies of those documents to SA Liv. They include a copy of BURKS's CDL and paystubs, a copy of his loan application, and a copy of the contract to purchase the 2012 BMW.

23. The contract appears to be dated February 23, 2018, and the loan application provides a month of February but the day is unclear. The CDL is the same as the one that BURKS provided to the Dodge Dealership. BURKS also listed the Long Beach Address as his residence, used the 8374 Social, and listed the same employer, Perpetual Holdings, Inc.

24. On or about August 28, 2018, SA Liv and I interviewed Tracey Kesterman, who is a Finance Director at Carson Honda. Kesterman told us that she received the car loan information the

day after the vehicle was purchased and sensed something was fraudulent about the information given. Despite that, Kesterman submitted BURKS's car loan application to Santander.

25. Santander rejected the loan because it could not verify BURKS's employment. On March 30, 2018, Santander notified its Fraud Investigation Department about BURKS's application. That department was initially concerned that the 8374 Social was linked to a synthetic identity. (I know from my training and experience that a synthetic identity refers to a false identification.) The Fraud Investigation Department determined that the 8374 Social belongs to a minor or recent immigrant. BURKS did not provide a copy of a social security card when he applied for the loan.

26. Because Santander rejected the loan application, Carson Honda contacted BURKS and requested that he return the 2012 BMW, which he did without incident.

27. I have reviewed the signatures on the loan application and sale contract for the purchase of the 2012 BMW and they appear to be identical to the signature on the CDL and to the signatures on the documents provided to the Dodge Dealership. Given that the dealerships did not report any discrepancy between the person who provided the CDL and the CDL, as well as that many of the items on the loan application sets forth information that is correctly associated with BURKS, I believe he is the person who applied for the loans for the 2012 and 2013 BMWs.

INVESTIGATION INTO BURKS'S ACTUAL IDENTITY AND LOCATION

BURKS's Actual SSN

28. Both SA Liv and I have used departmental resources to determine BURKS's actual SSN. Records show that it ends in 6083 (the "6083 Social"), which is different than the 8374 Social that he listed on his loan applications.

29. I checked a database connected to BURKS's state parole, which concluded in July 16, 2018, and learned that the SSN he provided is the 6083 Social, his true SSN.

30. On or about November 16, 2018, I received verification from the Social Security Administration that 8374 Social is a valid SSN and that it does not belong to BURKS.

BURKS'S EMPLOYMENT

31. On both loan applications, BURKS listed Perpetual Holdings Incorporated as his employer. BURKS attached pay stubs purported to be from Perpetual Holdings Inc. that showed $3,250.00, in gross pay for the pay period ending on February 20, 2018.

32. I conducted an investigation into Perpetual Holdings Inc. and it does not appear to be a currently operational company. I reviewed a document filed with the Court on September 5, 2015, regarding BURKS's release conditions, and it provides that BURKS and a friend founded Perpetual Holdings Incorporated in July 2015, to ease communication between inmates and their loved ones.

33. According to my investigation, Perpetual Holdings, Inc. was registered with the California Secretary of State on

July 29, 2015. BURKS is listed as the agent for service of process and the company's address is listed as 7833 Sepulveda Boulevard, Unit 38, Van Nuys, CA 91405 (the "Van Nuys Address").

34. The most recent date of any other filing with the California Secretary of State by Perpetual Holdings, Inc., was May 19, 2017. The California Secretary of State website lists the company's status as "FTB Suspended," which, the website explains means that "the business entity was suspended or forfeited by the Franchise Tax Board for failure to meet tax requirements (e.g., failure to file a return, pay taxes, penalties, interest)." The website does not provide the date of when Perpetual Holdings, Inc.'s status was suspended.

35. On November 27, 2018, I went to the Van Nuys Address but I saw no storefront or any indication that Perpetual Holdings, Inc. is operating there. I asked one of the store owners about Perpetual Holdings, Inc., and he said he was unfamiliar with that company but because there are a lot of small businesses there, I should speak to the manager. I left a message for the manager but have not heard back from that person.

36. On or about November 20, 2018, I conducted a search based on the 6083 Social through the California Employment Development Department regarding BURKS's employment. It provided that BURKS, for the first quarter of 2018, was employed at Jimenez V. Menzies Aviation Fund located at 50 Corporate Park, Irvine, California.

37. According to a report from SA Liv, prior to BURKS's employment at Jimenez V. Menzies Aviation Fund, his last employment was reported approximately at the end of December 2016, at Preferred Services Group LLC located at 401 W. Fallbrook Avenue, Suite 205, Fresno, CA 93711.

38. The parole database provides that BURKS "sells cars bought from auc," and I believe that "auc" stands for auction. There is no company name provided but the address for his place of employment is on Bixel Street, Los Angeles, CA 90017 (the "Bixel Address").

39. I believe, based on my training and experience and the investigation set forth above, that BURKS was likely not receiving a salary from Perpetual Holdings, Inc. at the time he applied for the car loans described above and that his assertions in the loan applications to the contrary were false.

INVESTIGATION INTO BURKS'S HOME ADDRESS

40. As noted above, BURKS listed the Long Beach address as his residence on his loan applications.

41. The database connected to BURKS's parole lists his home address as the Bixel Address (ostensibly, according to that database, also the address for his place of employment).

42. BURKS's CDL provides another address on Grace Avenue, Carson, California 90745.

43. Prior to obtaining the complaint, other law enforcement officers and I attempted to locate BURKS at each of the addresses associated with him and were unable to determine where he is living.

IDENTIFICATION OF THE SUBJECT PREMISES

44. Because I was unable to locate BURKS's residence, I obtained an arrest warrant for him, as described above. I then received legal authority to contact the United States Probation and Pre-trial Services unit ("Pretrial Unit") to obtain his address.

45. I then contacted the Pre-trial Unit, which provided BURKS's address as 900 West Temple Street, unit 528, Los Angeles, CA 90012, which is the SUBJECT PREMISES. BURKS updated his address in September 2018, which he is required to do as part of the conditions of his supervision. Additionally, BURKS is required to wear a GPS monitor while released on bond and must abide by a curfew that does not allow him to leave his residence between the hours of eleven pm and six am. The GPS monitor information, as provided to me by the Pretrial Unit, confirmed that between October 27, 2018 and December 4, 2018, BURKS has spent the night at the SUBJECT PREMISES.

V. TRAINING AND EXPERIENCE REGARDING FALSE STATEMENT TO A BANK, BANK FRAUD, AND IDENTITY THEFT

46. Based on my training and experience and information obtained from other law enforcement officers who investigate bank fraud, false statements to banks, and identity theft, I know the following:

a. It is common practice for individuals involved in bank fraud, false statement to a bank, and identity theft crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track

fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

c. Individuals who engage in bank fraud, false statement to a bank, and identity theft tend to possess documents and records reflecting their fraudulent activities, including bank account and credit card statements, loan application documents, business registration forms, genuine or fictitious income statements and tax records, receipts from

transactions and purchases, check images and copies, notes regarding their various accounts, wire transfer receipts, and communications regarding deposits, withdrawals, and transfers of funds. Such documents and records are generally maintained in places where individuals who engage in bank fraud, access device fraud, and identity theft can readily access them, often within those individuals' residences, in detached garages on their property, or on their person. Such documents and records are also often preserved in electronic form on digital devices in the possession of individuals who engage in the fraud.

d. Individuals who engage in bank fraud, false statement to a bank, and identity theft often communicate with others who aid, participate, or are involved in the same fraudulent activity. Such communications are often conducted and stored on digital devices. Additionally, individuals who engage in bank fraud, often maintain telephone numbers, email addresses, and other contact information for their co-conspirators. Such information is often stored on digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Such digital devices are generally maintained in places where individuals who engage in bank fraud, access device fraud, and identity theft can readily access them, often within those individuals' residences, in detached garages on their property, or on their person.

47. Individuals who engage in bank fraud, false statement to a bank, and identity theft tend to possess large quantities

of cash and tangible goods purchased using fraudulently obtained funds. Such large quantities of cash and tangible goods are generally maintained in places where individuals who engage in bank fraud can readily access them, often within those individuals' residences and in detached or attached garages on their property or are secured in safe deposit boxes or off-site locked storage facilities concealed from law enforcement. Individuals who engage in bank fraud may also take photographs or video of the proceeds of their fraud scheme and share the photos and video on their digital devices.

a. It is a common practice for those involved identity theft crimes to use either false identification or stolen real identification to make purchases with stolen access devices at retail stores in order to avoid detection and to complete the transaction. Those who engage in such fraud keep evidence of such retail transactions in their homes and cars.

b. Based on my training and experience, I know that individuals who participate in identity theft, false statement to a bank, and bank fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

48. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the

form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

49. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

50. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after

a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress BURKS's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of BURKS's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

51. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

52. For the reasons described above, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES or on BURKS's person.

AUNDRIA DAVIS LY, TFO
Federal Bureau of
Investigation

Subscribed to and sworn before me
this _____ day of January, 2019.

UNITED STATES MAGISTRATE JUDGE